Association for Information Systems
AIS Electronic Library (AISeL)

WISP 2015 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-13-2015

Development of the MyCyberSkills™ iPad App: A Scenarios-Based, Hands-On Measure of Non-IT Professionals' Cybersecurity Skills

Melissa Carlton
Nova Southeastern University

Yair Levy
Nova Southeastern University

Michelle Ramim
Hodges University

Steven Terrell
Nova Southeastern University

Development of the MyCyberSkills™ iPad App: A Scenarios-Based, Hands-On Measure of Non-IT Professionals' Cybersecurity Skills

Research in Progress

Melissa Carlton
Nova Southeastern University, USA {mc2418@nova.edu}

Yair Levy
Nova Southeastern University, USA {levyy@nova.edu}

Michelle M. Ramim
Hodges University, USA {mramim@hodges.edu}

Steven R. Terrell
Nova Southeastern University, USA {terrell@nova.edu}

ABSTRACT

Although advances in Information Technology (IT) have been significant over the past several decades when it comes to protection of corporate information systems (IS), human errors and social engineering appear to prevail in circumventing such IT protections. While most employees may have the best of intentions, without cybersecurity skills they represent the weakest link in an organization's IS security. Skills are defined as the combination of knowledge, experience, and ability to do something well. Cybersecurity skills correspond to the skills surrounding the hardware and software required to execute IS security to mitigate cyber-attacks. However, the current measures of end-user cybersecurity skills are based on self-reported surveys. This study is the second phase of a larger research project that is aimed to develop a scenario-based iPad application to measure cybersecurity skills based on actual scenarios with hands-on tasks that the participants complete in demonstrating their skills. To design a measure that has both high validity and reliability, subject matter experts' (SMEs) opinion of the top nine cybersecurity skills and their skill importance weight were identified in the first phase of the study following the Delphi method. This phase of the research in progress

Funding for this research was provided by the Nova Southeastern University's President's Faculty and Research Development Grant (PFRDG).

involves the design and development of the MyCyberSkills™ iPad application (app) using scenario-based, hands-on tasks related to each of the nine SMEs identified cybersecurity skills.

KEYWORDS: cybersecurity, cybersecurity skills, risk mitigation tool, information security skills of non-IT professional, design and development research

INTRODUCTION

Completing activities online are a part of everyday life, both professionally and personally. But, conducting business, interacting, and sharing information on the Internet does not come without its risks as well as potential for harm. Substantial information and financial losses for individuals, organizations, and governments are reported regularly due to vulnerabilities as well as breaches caused by insiders. Although advances in information technology (IT) have been significant over the past several decades when it comes to protection of corporate information systems (IS), human errors and social engineering appear to prevail in circumventing such IT protections. Even with the best intentions, IT users' mistakes, due to poor cybersecurity skills, represent the weakest link in an organization's IS security. Skills are defined as the combination of knowledge, experience, and ability to do something well. Furthermore, cybersecurity skills correspond to the skills surrounding the hardware and software required to execute IS security to mitigate cyber-attacks. To design a measure that has both high validity and reliability, the first phase of the study followed the Delphi method in seeking subject matter experts' opinion on the top platform independent cybersecurity skills for non-IT professionals (Carlton and Levy 2015). This study will facilitate an increase in the body of knowledge regarding non-IT professionals as it relates to their cybersecurity skills in the context of malware, personally identifiable information (PII), and work information systems (WIS) related threats. Moreover, it progresses the investigation of a valid problem statement with practical significance

(Terrell 2012). Thus, the aim of this study is to design and develop the scenario-based, hands-on tasks used to measure the cybersecurity skills level of non-IT professionals.

BACKGROUND

This research in progress is classified as developmental research. Developmental research tries to answer how the construction of a 'thing' addresses a problem (Ellis and Levy 2009). Richey and Klein defined developmental research as a way to "create knowledge grounded in data systematically derived from practice" (p. 1). According to Ellis and Levy, developmental research is comprised of three major elements: 1) product criteria is established and validated; 2) process for product development is accepted and formalized; as well as 3) determination of the product's criteria is met through a formalized, accepted process. In the work of Tracey and Richey, a systematic process was used to develop and then validate their model using the Delphi technique where an expert panel analyzed along with offering feedback on the proposed design. After suggested revisions were analyzed and incorporated, their model was validated by the Delphi technique (Tracey 2009). Thus, this study will design the scenarios-based, hands-on benchmarking index for measuring cybersecurity skills (Ramim and Lichvar 2014). Furthermore, the focus of this work will be on the measurement of non-IT professionals' demonstrated cybersecurity skills, not their behavior. Moreover, the main research question this study addresses is: What tasks will enable the validation of a hierarchical measure for observable cybersecurity skills of non-IT professionals?

METHODOLOGY

A hypothetical scenario method is "also known as a vignette or policy capturing method" (Siponen and Vance 2010 p. 492). With this method, each participant is presented with "written descriptions of realistic situations and then requested responses on a number of rating scales" (Trevino 1992 p. 127-128). Participants view scenarios as unintimidating and nonintrusive

(D'Arcy et al. 2009; Hu et al. 2011). Therefore, business, criminology, IS, and medical scholars have resorted to the use of scenarios to elicit input from participants (Hovav and D'Arcy 2012; Hu et al. 2011). A scenario method was the most used methodology in 55% of the 174 ethical decision-making articles reviewed by O'Fallon and Butterfield. Certification or specialist exams utilize a scenario-based and/or hands-on tasks to test the candidate's skills (Furnell 2004). Moreover, scenario-based assessments are utilized throughout industry and the military to measure skills (Thomas and Lee 2015; Wesolek 2009). Antisocial and ethical/unethical behavior assessment is commonly assessed with scenario-based methods (Siponen and Vance 2010). Consistent with prior IS research (e.g., D'Arcy et al. 2009; Hovav and D'Arcy 2012; Vance et al. 2012), the designed scenarios presented in this study represent realistic and commonplace situations to the participants.

Skill assessments are completed through the observation of demonstrated hands-on tasks (Vassiliou et al. 2014). Hands-on skill assessments are a substantial part of the medical academic communities (Berendonk et al. 2013). Transportation literature identifies scenarios as a method to measure a driver's skills without causing harm to individuals, damage to vehicles, or inaccurate self-perceived responses (Sahami and Sayed 2013; Sundström 2011). Moreover, aviation academic curriculum utilizes scenario-based, hands-on assessments to measure pilots' skills as mandated by the Federal Aviation Administration (Thomas and Lee 2015). The importance of skills and hands-on skills assessment found in the aviation, transportation, and healthcare industries appears applicable to cybersecurity skills as well. Torkzadeh and Lee used self-reported surveys to research the individual's perception of his or her skills and cautioned that perceived skills do not always correspond to actual skills. In the work of Gravill et al., users inaccurately assessed their knowledge of a specific software package. Prior literature addressed the flaws and consequences of erroneous self-assessment reporting (Mann 2010; Weigel and

Hazen 2014). Thus, this work will use scenario-based, hands-on tasks to assess the skills of non-IT professionals operationalized in the MyCyberSkills™ iPad app.

The results of phase one provided a foundation in achieving the designed set of observable hands-on, scenarios-based tasks that measure cybersecurity skills of non-IT professionals without the bias of or need for self-assessment (Carlton and Levy 2015). Table 1 displays the cybersecurity skills index (CSI), the SMEs ranked cybersecurity skills (SK_i), their respective hands-on tasks (T_{i_j}), description, range, and weight. Each skill was designed in this study to include a group of four cybersecurity related hands-on tasks for the non-IT professional to identify and demonstrate their skill level as if in a real-life situation (Hovav and D'Arcy 2012; Vance et al. 2012). The sum of all nine skills multiplied times their respective weight (w_i) is then multiplied times the coefficient of $\left(\frac{5}{2}\right)$. This results in the non-IT professionals' CSI score of 0 to 100. With the use of literature, (e.g., Glazer and Yadron 2014), a scenario begins each task.

Table 1: Cybersecurity Skills Index and SMEs Ranked Cybersecurity Skills

Variable	Components	Description	Range	Weight
SK_1	$T_{1_1} + T_{1_2} + T_{1_3} + T_{1_4}$	Preventing the leaking of confidential digital information to unauthorized individuals	0 – 40	.136
SK_2	$T_{2_1} + T_{2_2} + T_{2_3} + T_{2_4}$	Preventing malware via non-secure Websites	0 – 40	.132
SK_3	$T_{3_1} + T_{3_2} + T_{3_3} + T_{3_4}$	Preventing personally identifiable information (PII) theft via access to non-secure networks	0 – 40	.127
SK_4	$T_{4_1} + T_{4_2} + T_{4_3} + T_{4_4}$	Preventing PII theft via e-mail phishing	0 – 40	.112
SK_5	$T_{5_1} + T_{5_2} + T_{5_3} + T_{5_4}$	Preventing malware via e-mail	0 – 40	.109
SK_6	$T_{6_1} + T_{6_2} + T_{6_3} + T_{6_4}$	Preventing credit card information theft by purchasing from non-secured Websites	0 – 40	.100
SK_7	$T_{7_1} + T_{7_2} + T_{7_3} + T_{7_4}$	Preventing information system compromise via USB or storage drive/device exploitations	0 – 40	.097
SK_8	$T_{8_1} + T_{8_2} + T_{8_3} + T_{8_4}$	Preventing unauthorized information system access via password exploitations	0 – 40	.095
SK_9	$T_{9_1} + T_{9_2} + T_{9_3} + T_{9_4}$	Preventing PII theft via social networks	0 – 40	.092
CSI	$\left(\frac{5}{2}\right)\sum_{i=1}^{9}[(SK_i) \cdot w_i]$	Coefficient * (Sum of all 9 skills * respective weights)	0 – 100	

Once task one of a skill is completed, scenario two is presented. Task two then increments in difficulty and presents the non-IT professional again with four response options. This presentation continues measuring the non-IT professionals' skills with an easy, somewhat

difficult, difficult, and very difficult task within each skill. Appendix A illustrates the process of each skill (n) as it is presented to the non-IT professional. Each skill begins with a scenario (i.e., n.1), then presents the hands-on task with four response options (i.e., n.1.1). For some skills, the individual's response warrants an alternate scenario for maintaining the incremental level of difficulty. When this occurred, scenarios were identified as A and B as seen in the somewhat difficult category of appendix A.

MyCyberSkills™ iPad APPLICATION DEVELOPMENT

While the development and validation of a comprehensive set of scenario-based, hands-on benchmarking index is a good step in the right direction, the process of implementing it in order to actually measure such skills can be challenging. In order to overcome this issue, the MyCyberSkills™ iPad application (app) prototype operationalizes the previously developed and validated scenarios-based, hands-on benchmarking index into an iPad app that will be used to assess the cybersecurity skills of non-IT professionals. The conceptual design of the CSI as it is presented within the MyCyberSkills™ iPad app prototype is exhibited in Figure 1.

Figure 1: Conceptual Design of the MyCyberSkills™ iPad App

The written scenario-based, hands-on tasks are transformed into a digital presentation with the use of Articulate Storyline 2. Figure 2 illustrates the home screen of the MyCyberSkills™ iPad app prototype. Appendix B includes screen shots from the designed scenarios-based, hands-on tasks of a skill and the respective developed screen shots for

presentation within the prototype. Each of the cybersecurity related tasks are presented individually in the MyCyberSkills™ prototype. As the non-IT professional responds to each hands-on observable task, the MyCyberSkills™ prototype records the non-IT professional's performance level using a scale of 0 to 10 and then presents the next cybersecurity related task. According to Schwartz and Fischer, an individual cannot solve a problem that exceeds the individual's highest developed skill level. Therefore, the level of difficulty increases as each task is presented within the respective skill. Once the set of tasks for a specific skill is completed by the non-IT professional, the next set of tasks begin with a relevant scenario followed with the least difficult cybersecurity related tasks and incrementing to the most difficult cybersecurity related tasks. This process continues until a response is received for each task. Figure 3 illustrates the achieved overall CSI and the individual cybersecurity skill scores.

Figure 2: Home Screen of MyCyberSkills™ Skills Prototype

Figure 3: Individual Cybersecurity and Overall CSI Scores

FUTURE WORK

To ensure the validity and reliability of the MyCyberSkills™ iPad app prototype, rigorous testing will be completed throughout the development process. After obtaining Institutional Review Board (IRB) approval to work with human subjects, stability and internal consistency will be documented through a pilot study consisting of non-IT professionals. As the scenarios-based, hands-on tasks are developed, each response will be given a score. To ensure

the correct score is recorded and each participant receives an accurate CSI score by the MyCyberSkills™ iPad app, 10 non-IT professionals will be observed while demonstrating their hands-on tasks during the pilot-test of the initial app prototype testing. As the participants demonstrate each task, the action taken will be both automatically and manually recorded, while both recordings will be compared for additional validation testing. Moreover, the individual task scores, the overall score for each skill, and the CSI score will be validated using this process. Additionally, validity will be tested by asking for SMEs' comments as well as suggestions to ensure the prototype maintains consistency and internal validity when measuring the skills via the scenarios-based, hands-on tasks (Ramim and Lichvar. 2014). Revisions to the MyCyberSkills™ iPad app prototype will be made prior to the empirical study (Sheng et al. 2007; Terrell 2012). After the revisions are completed, an empirical study will be conducted using the developed and validated MyCyberSkills™ prototype with a larger group of non-IT professionals. Furthermore, recommendations based on the empirical data from the MyCyberSkills™ iPad app prototype will be provided to c-level executives on the 'at risk' group of employees that may require further cybersecurity training.

REFERENCES

Berendonk, C., Stalmeijer, R. E., and Schuwirth, L. W. 2013. "Expertise in performance assessment: Assessors' perspectives," *Advances in Health Sciences Education* (18:4), pp. 559-571.

Carlton, M., and Levy, Y. 2015. "Expert assessment of the top platform independent cybersecurity skills of non-IT professionals," *Proceedings of the 2015 IEEE SoutheastCon,* Ft. Lauderdale, Florida, pp. 1-6.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach," *Information Systems Research* (20:1), pp. 79-98.

Ellis, T. J., and Levy, Y. 2009. "Towards a guide for novice researchers on research methodology: Review and proposed methods," *Issues in Informing Science and Information Technology* (6), pp. 323-337.

Furnell, S. 2004. "Qualified to help: In search of the skills to ensure security," *Computer Fraud and Security* (2004:12), pp. 10-14.

Glazer, E., and Yadron, D. 2014, October 2. "J.P. Morgan says about 76 million households affect by cyber breach," *The Wall Street Journal, Markets*. (available at http://online.wsj.com/articles/j-p-morgan-says-about-76-million-households-affected-by-cyber-breach-1412283372).

Gravill, J. I., Compeau, D. R., and Marcolin, B. I. 2006. "Experience effects on the accuracy of self-assessed user competence," *Information and Management* (43:3), pp. 378-394.

Hovav, A., and D'Arcy, J. 2012. "Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea," *Information and Management* (49:2), pp. 99-110.

Hu, Q., Xu, Z., Dinev, T., and Ling, H. 2011. "Does deterrence work in reducing information security policy abuse by employees?" *Communications of the ACM* (54:6), pp. 54-60.

Mann, K. V. 2010. "Self-Assessments: The complex process of determining 'how we are doing' – a perspective from medical education," *Academy of Management Learning and Education* (9:2), pp. 305-313.

O'Fallon, M. J., and Butterfield, K. D. 2005. "A review of empirical ethical decision-making literature: 1996-2003," *Journal of Business Ethics* (59:4), pp. 375-413.

Ramim, M. M., and Lichvar, B. T. 2014. "Eliciting expert panel perspective on effective collaboration in system development projects," *Online Journal of Applied Knowledge Management* (2:1), pp. 122-136.

Richey, R. C., and Klein, J. D. 2014. "Design and development research," in *Handbook of Research on Educational Communications and Technology*, J. M. Spector, M. D. Merrill, J. Elen, and M. J. Bishop (eds.), New York: Springer, pp. 141-150.

Schwartz, M. S., and Fischer, K. W. 2004. "Building general knowledge and skill: Cognition and microdevelopment in science learning," in *Cognitive developmental change: Theories, models, and measurement*, A. Demetriou and A. Raftopoulos (eds.), Cambridge, U. K.: Cambridge University Press, pp. 157-185.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., and Cranor, L. F. 2007. *Anti-Phishing Phil: The design and evaluation of a game that teaches people not to fall for phish*. (available at http://repository.cmu.edu/isr/22/).

Siponen, M., and Vance, A. 2010. "Neutralization: new insights into the problem of employee information systems security policy violations," *MIS Quarterly* (34:3), pp. 487-A12.

Sahami, S., and Sayed, T. 2013. "How drivers adapt to drive in driving simulator, and what is the impact of practice scenario on the research?" *Transportation Research Part F: Traffic Psychology and Behaviour* (16), pp. 41-52.

Sundström, A. 2011. "The validity of self-reported driver competence: Relations between measures of perceived driver competence and actual driving skill," *Transportation Research Part F: Traffic Psychology and Behaviour,"* (14:2), pp. 155-163.

Terrell, S. 2012. *Statistics translated: A step-by-step guide to analyzing and interpreting data*, New York, NY: The Guilford Press.

Thomas, R., and Lee, C. C. 2015. Development of training scenarios in the flight training device for flight courses at Embry-Riddle Aeronautical University," *Journal of Aviation/Aerospace Education & Research* (24:3), pp. 65-82.

Torkzadeh, G., and Lee, J. 2003. "Measures of perceived end-user computing skills," *Information and Management* (40:7), pp. 607-615.

Tracey, M. W. 2009. "Design and development research: A model validation," *Educational Technology, Research and Development* (57:4), pp. 553-571.

Tracey, M. W., and Richey, R. C. 2007. "ID model construction and validation: A multiple intelligences case," *Educational Technology, Research and Development* (55:4), pp. 369-390.

Trevino, L. K. 1992. "Experimental approaches to studying ethical-unethical behavior in organizations," *Business Ethics Quarterly* (2:2), pp. 121-136.

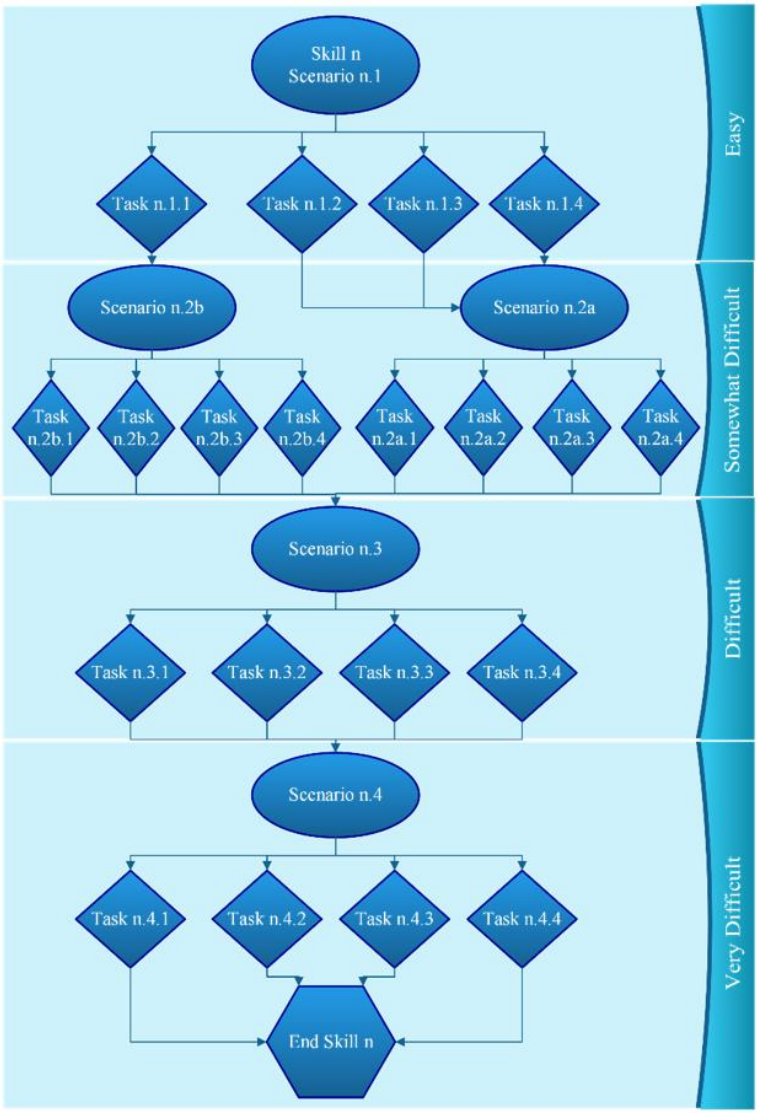
Vance, A., Siponen, M., and Pahnila, S. 2012. "Motivating IS security compliance: Insights from habit and protection motivation theory," *Information & Management* (49:3), pp. 190-198.

Vassiliou, M., Dunkin, B., Fried, G., Mellinger, J., Trus, T., Kaneva, P., Lyons, C., Korndorffer, J., Ujiki, M., Velanovich, V., Kochman, M., Tsuda, S., Martinez, J., Scott, D., Korus, G., Park, A., and Marks, J. (2014). Fundamentals of endoscopic surgery: creation and validation of the hands-on test. *Surgical Endoscopy* (28), 704-711.

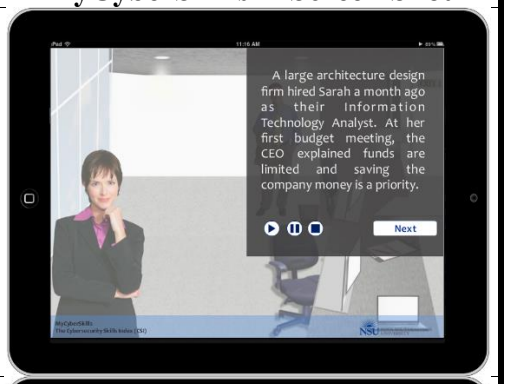
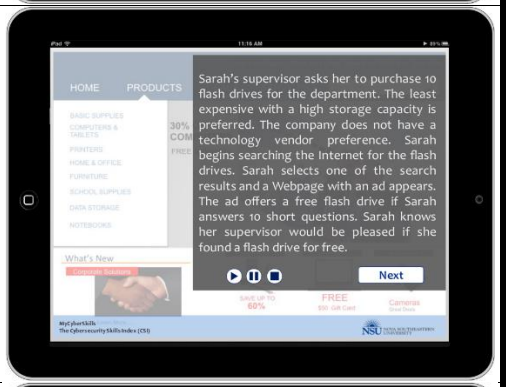
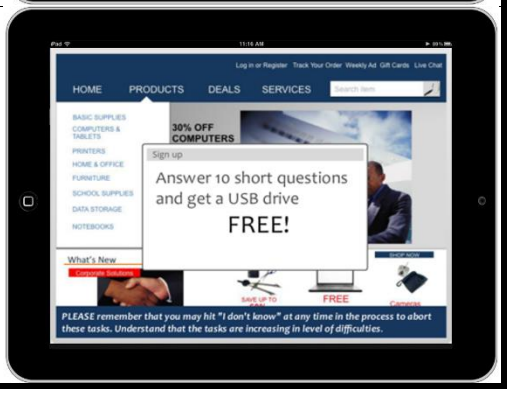
Weigel, F. K., and Hazen, B. T. 2014. "Technical proficiency for IS success," *Computer in Human Behavior* (31), pp. 27-36.

Wesolek, M. L. 2009. "Analysis of the effectiveness of Army helicopter flight training," *Journal of Aviation/Aerospace Education & Research* (18:2), pp. 69-87.

APPENDIX A: Scenario-Based, Hands-On Task Skill Levels

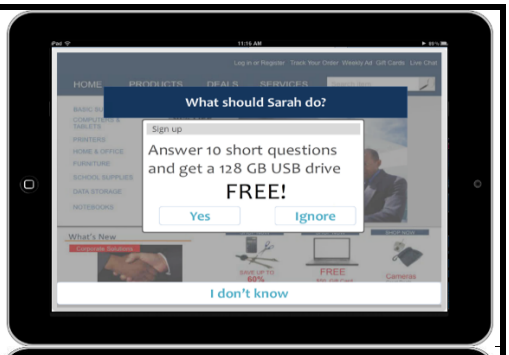


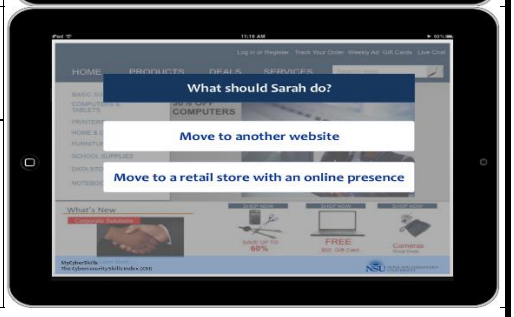
APPENDIX B: Scenario-Based, Hands-On Task and Its MyCyberSkills™ Presentation

Designed Written Scenarios-based, Hands-on Tasks	Respective Developed MyCyberSkills™ Screen Shot
Scenario n.1: A large architecture design firm hired Sarah a month ago as their Information Technology Analyst. After her first budget meeting, the CEO explained funds are limited and saving the company money is a priority.	
Sarah's supervisor asks her to purchase 10 flash drives for the department.	
The least expensive with a high storage capacity is preferred. The company does not have a technology vendor preference. Sarah begins searching the Internet for the flash drives.	
Sarah selects one of the search results and an ad on the Webpage appears. The ad offers a free flash drive if Sarah answers 10 short questions. Sarah knows her supervisor would be pleased if she found a flash drive for free. Present the user with a Banner AD instructing people to answer 10 short questions and in return get a 128GB USB drive free	

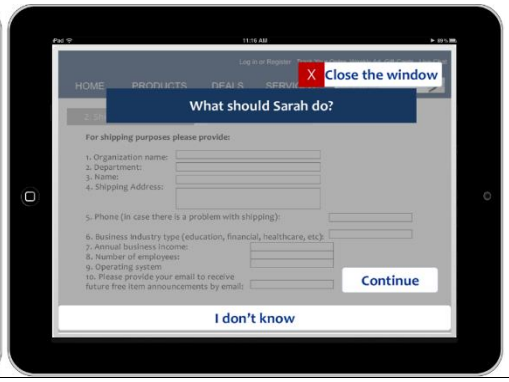
Task: What should Sarah do?

Option	Framed Action	Description	What happens	Score
n.1.1	Yes	Click on the Banner Ad to proceed further	takes user to screen 2.2b	0
n.1.2	I don't know	Aborts the task	takes user to screen 2.2a	2
n.1.3	Ignore	• Move to a different website	takes user to screen 2.2a	6
n.1.4		• Move to a retail store with an online presence	takes user to screen 2.2a	10





Move to another website screenshots



Move to a retail store with an online presence screenshots